Autorisation & Contrôle d’Accès

Stratégies, standards, sécurité...

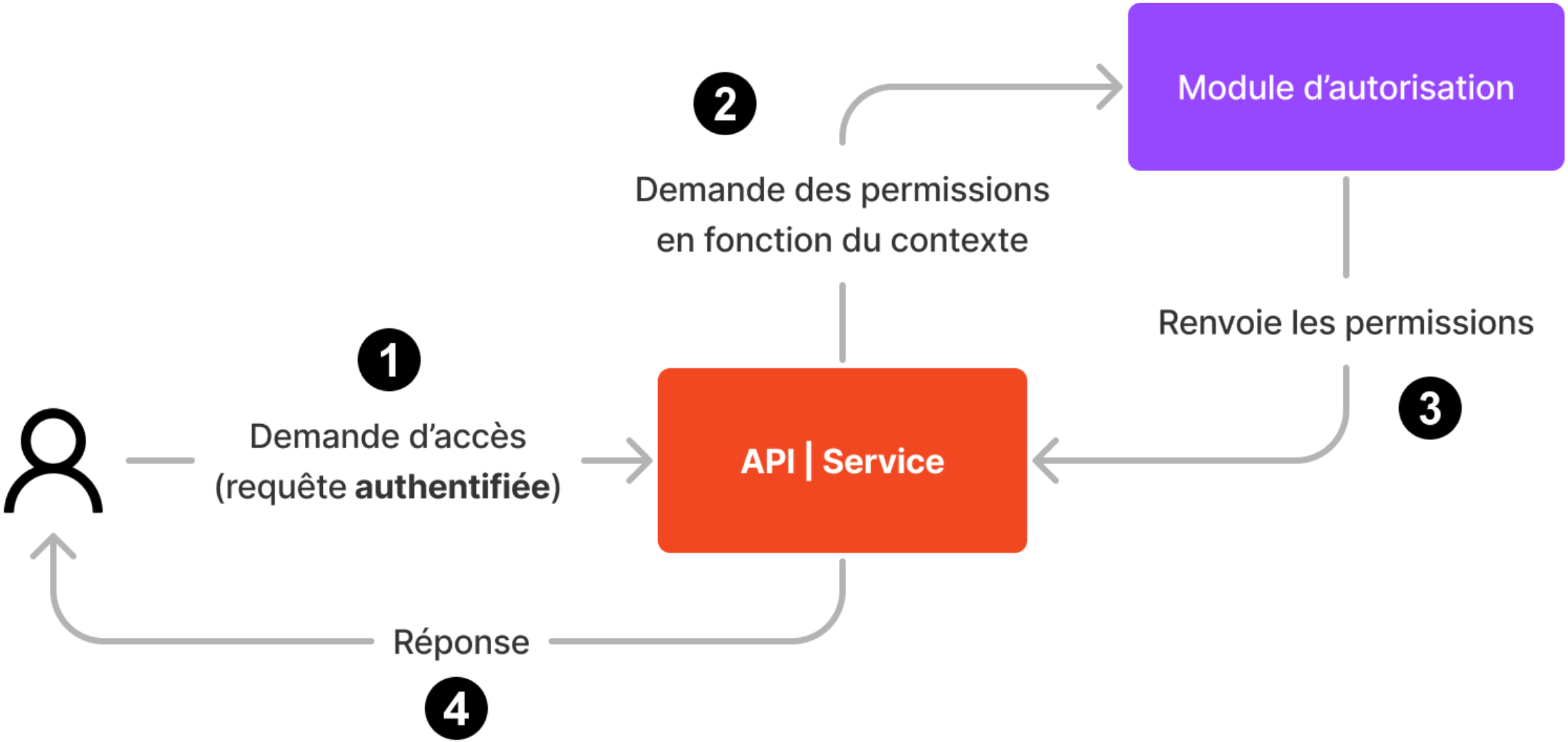
Définitions

Identification	Action de fournir une preuve de son identité.
Authentification (AuthN)	Vérification de l'identité. La demande est-elle légitime ?
Autorisation (AuthZ)	Action de déterminer ce que l'entité **peut** faire.
Contrôle d'Accès (AC)	Mécanisme complet (Identification + AuthN + AuthZ).

 **IMPORTANT** 

AuthZ

Processus permettant de déterminer les **droits** d'une entité (personne, système) sur des ressources

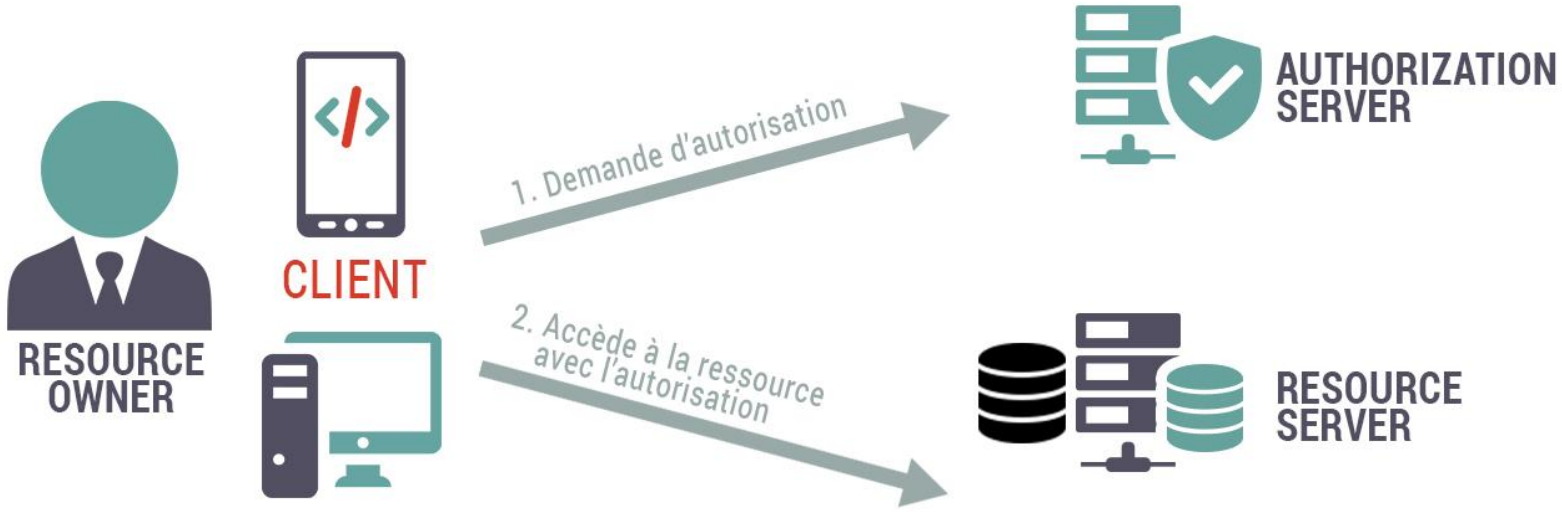

Module d’autorisation
2
Demande des permissions
en fonction du contexte
Renvoie les permissions
3
1
Demande d’accès
(requête **authentifiée**)
API | Service
Réponse
4

Niveaux de contrôle d'accès

Type	Niveau	Description	Exemple
Basé sur les rôles (RBAC)	Rôle (groupe)	Les droits sont accordés en fonction des rôles du sujet. Un rôle permet de regrouper un ensemble de permissions.	Le sujet est un **administrateur**, alors il a le droit de suppression sur **toutes** les ressources.
Basé sur les attributs (ABAC)	Sujet (individu)	Les droits sont accordés en fonction des attributs du sujet.	L'**âge** du sujet est **d'au moins 18 ans**, alors il a le droit de commander de l'alcool.
Basé sur les relations (ReBAC)	Utilisateur ET ressource (contexte précis)	Les droits sont accordés en fonction des relations entre le sujet et une ressource.	Le sujet a le droit de supprimer **ce** post car **il lui appartient**. *Il existe une **relation** d'appartenance entre le post et le sujet.*

Oauth 2.0

Protocole de « délégation d'autorisation » **(et non pas d'authentification !)** autorisant un **consommateur** (site web, application, ...) à utiliser l'API d'un **fournisseur** (autre site web, service) pour le compte d'un **utilisateur**



OpenIDConnect

- Couche d'authentification **basée sur OAuth 2.0**
- Permet aux clients de vérifier l'identité d'un utilisateur final
- **Standard industriel** utilisé par Google, Microsoft, Facebook...

SSO (Single Sign-On)

- Permet à l'utilisateur d'accéder à **plusieurs** services et applications en ne procédant qu'à **une seule authentification**
- Utilise très souvent OpenIDConnect qui est prévu à cet effet